NAVAL WAR COLLEGE
Newport, R.I.

TECHNOLOGY IN TRANSFORMATION: CRITICAL STRENGTH OR CRITICAL VULNERABILITY?

By

David R. Price
Commander, U.S. Navy

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:_____

18 May 2001

_____
Faculty Advisor: CAPT J. T. Locks, USN

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
18052001	N/A	-

Title and Subtitle Technology in Transformation: Critical Strength or Critical Vulnerability?	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Price, David R.	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Naval War College 686 Cushing Road Newport, RI 02841-1207	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 26	

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol:
C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):
Technology in Transformation: Critical Strength or Critical Vulnerability?
(UNCLAS)

9. Personal Authors: David R. Price, CDR, USN

10.Type of Report: FINAL

11. Date of Report: 18 May 2001

12.Page Count: 22 **12A Paper Advisor (if any): J. T. Locks, CAPT, USN**

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: defense transformation, information technology, center of gravity, training, organization, logistics, interoperability

15.Abstract: Technologies the U.S. military depends on are at risk of failing during the on-going transformation of the joint force. The transformation process itself results in vulnerabilities including logistic support, interoperability, and training, which increase the risks of technology failure. Driving forces behind these vulnerabilities include: societal desire for, and belief in technology; political considerations; budget limitations; market forces; and competent potential adversaries. The warfighting CinCs can mitigate the risks of technology failure associated with transformation with an approach that includes: preventing the premature deployment of weapon systems; training assigned forces for general technology failure; and reorganization of the command and control structure to support decentralized execution and self-synchronization.

16.Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461 **20.Office Symbol: C**

Security Classification of This Page Unclassified

ABSTRACT

Technologies the U.S. military depends on are at risk of failing during the on-going transformation of the joint force. Driving forces behind how the military transforms its forces include: societal desire for, and belief in, technological solutions; political impetus to develop and field increasingly complex technologies; a constrained top-line budget forcing zero-sum decisions within the government; market forces resulting in the world-wide proliferation of technology; and competent adversaries who will create a technology-hostile battlespace. Complicating the transformation process are elements, which, if left unattended, lead to critical vulnerabilities. These include human-technology relationships, logistic support, interoperability, training and budget decisions. The warfighting CinCs can mitigate the risks of technology failure associated with transformation with an approach that includes: preventing the premature deployment of weapon systems; training assigned forces for general technology failure; and reorganization of the command and control structure to support decentralized execution and self-synchronization.

BIBLIOGRAPHY

Alberts, David S., John J. Garstka, Frederick P. Stein. Network Centric Warfare. Washington, DC: CCRP, 1999.

Biddle, Stephen, Wade P. Hinkle and Michael P. Fischerkeller, "Skill and Technology in Modern Warfare." Joint Forces Quarterly (Summer 1999): 18-27.

Budiansky, Stephen. "The Physics of Gridlock." The Atlantic Monthly (December 2000): 20-24

Cebrowski, Arthur K. and John J. Garstka. "Nework-Centric Warfare—Its Origin and Future." U.S. Naval Institute Proceedings (January 1998): 28-35.

Dumond, John, Rick Eden, Douglas McIver and Hyman Shulman. Maturing Weapon Systems for Improved Availability at Lower Costs. Santa Monica, CA: RAND, 1994.

Gompert, David C. and Irving Lachow. "Transforming U.S. Forces: Lessons from the Wider Revolution." Lkd. Online RAND Research Documents at "Military Force Structure and Employment" page. < http://www.rand.org/publications/electronic/force.html> [10 Apr 2001].

Guthrie, Neale D., "The Impact of Technological Change on Military Manpower in the 21st Century." thesis, Naval Postgraduate School, 1990.

Herman, Mark. "Entropy-Based Warfare: Modeling the Revolution in Military Affairs." Joint Forces Quarterly. (Autumn/Winter 1998-99), 85-90.

Joint Military Operations Department, Syllabus and Study Guide for Joint Military Operations. Newport, RI: Naval War College, 2001.

Lescher, William K. "Network Centric: Is It Worth the Risk?" U.S. Naval Institute Proceedings (July 1999): 58-63.

Lieberman, Joseph I. "Techno-Warfare; Innovation and Military R&D." Joint Forces Quarterly, (Summer 1999): 13-17.

Murdock, Paul. "TAOs Must Fight at the Operational Level," U.S. Naval Institute Proceedings (January 2001), 86-87.

National Intelligence Council, Global Trends 2015: A Dialogue About the Future with Nongovernment Experts. December 2000.

Naval War College Faculty. Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age. Smooth Draft. Newport, RI: Naval War College, 2000.

Novak, Linda A., Drazek, Gregory P. and Stimatze, Gregg L. Logistics Technology 2010; Implications for DOD. Mclean, VA: Logistics Management Institute, December 2000.

Perry, Walter L., Bruce R. Pirnie and John V. Gordon IV. Issues Raised During the Army After Next Spring Wargame. Santa Monica, CA: RAND, 1999.

Schwartz, Peter. The Art of the Long View. New York: Doubleday, 1991.

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." Parameters. (Spring 2000): 13-29.

U.S. Department of the Army. Weapon Systems 1986. Washington, DC: 1986.

_____. Weapon Systems 2000. Washington, DC: 2000.

U.S. Joint Chiefs of Staff. Joint Vision 2020. Washington, DC: June 2000

U.S. Joint Chiefs of Staff. National Military Strategy of the United States of America. Washington, DC: 1997.

U.S. President. A National Security Strategy for a Global Age. Washington, DC: The White House, December 2000.

Vego, Milan N. Operational Warfare. Newport, RI: Naval War College, December 2000.

Zimm, Alan D. "Human-Centric Warfare," U.S. Naval Institute Proceedings (May 1999): 28-31.

TECHNOLOGY IN TRANSFORMATION: CRITICAL STRENGTH OR CRITICAL VULNERABILITY?

> In generic terms, a center of gravity (COG) is that source of massed strength – physical or moral, or a source of leverage – whose serious degradation, dislocation, neutralization, or destruction would have the most decisive impact on the enemy's or one's own ability to accomplish a given military objective.
>
> Milan Vego, *Operational Warfare*[1]

Introduction

The U.S. military's infatuation with technology and preference for technological solutions to problems have created vulnerabilities that can be exploited by an adversary. This is especially so during the on-going defense transformation when economic considerations have driven us to abandon less complex backups and the training necessary to successfully continue operations in the face of technology failures. Since the Services lack the money to prepare for technological failure, the warfighting commanders in chief (CinCs) are left with an unbalanced force during transformation, one extremely dependent on technologies that are at risk of failure.

Joint Vision 2020 states the transformation's goal as "the creation of a force that is dominant across the full spectrum of military operations."[2] By design the transformation process is intended to answer most of the technical, organizational and educational requirements of the future joint force. The process itself, however, presents risks of general technological failures, which our operational-level warfighters must be able to manage. The transformation process, intended to capitalize on our technological superiority as a critical strength, instead results in several critical vulnerabilities, including: more expensive and complex training and logistic support requirements; technology barriers to interoperability with existing systems; and overconfidence on the part of our political leadership, the public and even the military with respect to our capabilities. Left unattended, these vulnerabilities increase the probability of technological failure during the transformation period and amplify the effects of such failures. [3]

We can and should prepare for the vulnerabilities inherent in transformation, however unlikely they might seem from our current technologically superior vantage point. Our warfighters must be capable of continued operations without some elements of our technology. Information systems, the Global Positioning System (GPS), and satellite communications exemplify elements of our technological superiority, which, if they fail, impact a force at every level, making it difficult or impossible to continue operations. If the network in Network Centric Warfare (NCW) goes down, or an adversary strikes GPS before we have made it robust and survivable, or the communications in our hierarchical command structure are muted, we still need to be able to fight and win. Military engagements for minor interests during the transformation give us the luxury of withdrawing due to technological failure, if necessary, with only our prestige and credibility damaged. But withdrawal may not be an option if vital national interests are at stake, even if that withdrawal is dictated by a system-wide technological failure.

During the transformation to the joint force of 2020, our forces will likely be called on to conduct operations at least as large as our recent forays into the Balkans. If conflicts involving our national interests occur, we will have to fight and win, in whatever state of transformation we find ourselves. We will also continue to face uncertainty, in light of which we should develop worst-case scenarios of critical technology failure in order to prepare for lesser cases of failure.[4] Critical technologies are those upon which we have become dependent to the point they represent critical vulnerabilities. Though addressing specific systems is beyond the scope of this paper, we can identify factors during transformation that increase the vulnerability of our technologies and then consider operational level courses of action to mitigate the associated risks.

Transformation Gridlock: A Scenario for Technological Failure

In building a scenario for technological failure, one can liken the transformation process to the flow of traffic on our streets and highways. There are large forces that control the general rate and direction of flow, and lower-level perturbations that affect the flow. The flow is slowed by either self-induced (predictable but overlooked) or chaotic (unpredictable) perturbations, similar to traffic jams. When not managed properly (systemically), the flow can become restricted to the point of "gridlock," with a resulting increased risk of general technology failures.[5] For example, fielding a new system before the compatibility and logistics issues of previous generations have been addressed slows the overall flow of transformation. As more systems are added, the interoperability and logistics problems compound, cascading into transformation gridlock, in which it is impossible to fully address the issues of any fielded system due to budget constraints. Eventually readiness falls and the only way out of the downward spiral is a combination of increased spending and halting new systems introductions, while those in place are either matured or retired.

The first step in building the transformation scenario is to identify driving forces and sources of perturbations in the transformation flow. In his book *The Art of the Longview*, Peter Schwartz lists several driving forces that apply to building a scenario. These include society, economics, politics, and environment; each has a role in a transformation scenario in which technology is a critical vulnerability.[6]

Societal factors play a large role in the goal of military transformation, especially in today's information age. Americans have always loved technological solutions to complicated problems. There is something powerful about using complex tools to modify one's environment or improve one's capabilities. The information age has only amplified this. We are obsessed with

the wonderful consumer electronic devices used to connect, entertain and inform us. Our way of war reflects this, multiplied by several orders of magnitude. As an example of how the information age has affected the growth of technology in the military, one need only compare the US Army's annual *Weapon Systems* books. In 1986 the book was introduced with: "The US Army is in the midst of the largest peacetime modernization program in our nation's history." Only 17 programs detailed that year were information-type systems. The total number of information-type systems cited in the 2000 version was 69![7] We have raised the ante on what can be called a large modernization program, with the associated increased "traffic" on our transformation "highway," and this just from the Army, our least technology-oriented service.

Economics is the key driving force in the transformation scenario. Without a direct, immediate and obvious threat to our national security, it is unlikely that the top line in military spending will increase from the current level. It would be nice if Congress increased the defense budget but we should not plan on such an increase. Instead, a fixed budget should be assumed and can be thought of as the width of the transformation "highway," creating a zero-sum game, in which every choice results in a tradeoff or opportunity cost. Fielding and supporting one program comes at either the expense of another program, the rate at which transformation proceeds, or the training and support for an existing program.

Zero-sum choices raise the stakes for those who support programs, accentuating another driving force, politics. The transformation of our military forces during the next fifteen to twenty years will not be a smooth and orderly process. Complicating the rate and direction of the transformation are political conflicts of interest. Natural in our form of government, they will prevent us from quickly transforming our forces, likely extending the transformation well beyond 2020, and perhaps yielding a completely different goal from that envisioned today.

Competing interests will be addressed, some of which will not be directly or even recognizably related to national security. The result could be the continued proliferation of service-specific or even community-specific technologies that diverge from the desired joint technology toward which our transformation forces are supposed to be moving.

One should expect that our transformation technologies will operate in an environment less cooperative than anything we've seen since the end of the Cold War. Unlike our post-Cold War engagements in the Middle East and Balkans, we should not expect to encounter adversaries who are nearly impotent in the face of our technology. "Adversaries will seek to attack US military capabilities through electronic warfare, psychological operations, denial and deception, and the use of new technologies such as directed energy weapons or electromagnetic pulse weapons. The primary purpose would be to deny US forces information superiority, to prevent US weapons from working, and to undermine US domestic support for US actions."[8]

Despite optimistic visions of total battlespace awareness and full-spectrum dominance, US superiority is not a forgone conclusion, especially during the transformation period. Though our technological advantage is unquestioned today, in creating a transformation scenario we should plan for confronting an adversary who is able sometimes to effect major damage to our information and command and control (C2) systems. This is a reasonable expectation given the market forces that steadily make technology, and the ability to defeat it, cheaper and more accessible to potential adversaries. Our capitalist system has an inherent conflict of interest between peacetime economic growth and the retention of wartime advantages.[9] This manifests itself in overseas technology sales to potential military competitors. Information technology is widely available and serves both military and peaceful purposes, undermining our military's technological superiority. Additionally, the fact that our military is a relatively small consumer

of high-tech products (specifically information systems) compared with the global private sector makes it even more difficult for us to maintain our technological advantage. We stifle technology sales only at some risk to our national economic health. We cannot protect information technology as if it were akin to the Manhattan Project; the proverbial genie is out of the bottle.

The technologies we depend on have not yet been tested under the fire of a competent adversary who has the ability to target them. Arguably, we have not faced a peer force since Korea. Our victories in Kuwait and Kosovo should not be considered laurels on which to rest our case for technological superiority. The need for lopsided expenditures to win in such engagements should be cause for concern, not pride. We should hope the need for such huge spending ratios between an opponent and us do not hold true for future conflicts, especially conflicts with forces better prepared to give us a fight.

In summary, driving forces of the transformation scenario include:

- Societal desire for technological solutions.
- Political impetus to develop and field increasingly complex technologies.
- A constrained top-line budget forcing zero-sum decisions within the government.
- Market forces resulting in the world-wide proliferation of technology.
- Competent adversaries who will create a technology-hostile battlespace.

Traffic Jams on the Transformation Highway

The recent rash of peacetime accidents can be likened to fender-benders in the traffic analogy suggested above. The closer we come to gridlock, the more frequent, and deadly, these accidents become. But V-22 crashes, submarine collisions or other front-page incidents are only symptoms of impending gridlock. Though these are the most obvious signs of failure, they are

isolated incidents and can actually obscure the underlying problems associated with the transformation. They present situations in which it is easy to lay blame at lower-level causes immediate and specific to each incident, diverting attention from the root causes of failure.

Schwartz refers to "predetermined elements" and "critical uncertainties" in the scenario building process. Predetermined elements are independent of other events and are certain to be present no matter how a scenario evolves.[10] Critical uncertainties are based on the interaction of these elements within the scenario and result in a range of possible impacts, from minor delays to full-fledged gridlock. We are uncertain of the result due to the number of variables and elements involved in the scenario. As the flow through our high-tech acquisition, fielding and operations highway becomes restricted, failures can become more widespread, perhaps involving entire systems or major subsystems, resulting in operational failure during conflict. Looking at predetermined elements associated with the transformation process may provide insight into how those elements contribute to failures, guiding us in shifting resources or attention in time to prevent (or live with) failures. For the purpose of this scenario of technology vulnerability during transformation, relevant predetermined elements are those that contribute to vulnerability and should therefore be planned for in managing the transformation. Among these elements are: human-technology relationships; logistics, interoperability and training problems inherent to transformation; and the budget.

The GPS Effect: Human-Technology Relations

Our doctrine has an underlying tone of optimism regarding the inevitability of success. Over-confidence in technology has led to increased dependence on, and planned human force reductions based on, capabilities that have not yet matured. This over-confidence permeates our armed forces at every level; we remain unaware of the risks of failure of our technology, and

untrained for the consequences. An example of over-confidence is GPS, on which we have based more and more complicated information and weapons systems, with the apparent certainty it will never fail, despite its generally acknowledged susceptibility to simple jamming techniques. We apparently cannot even consider the possibility of failure of a technology on which we are so dependent. Instead it is easier to assume we WILL have technological superiority, it WILL give us intimate knowledge of the battle space, it WILL get us inside the decision loop of the enemy, and it WILL result in massed effects from great distances with few casualties by even fewer human forces. It will, in effect, trump the fog and friction of war. Of course, even if all this is possible, it will only be after the transformation is complete.[11]

The Traffic: Logistics, Training and Interoperability

The existence of legacy systems in our defense hardware inventory will never change, though their impact might be mitigated by more backward-compatible and upgradeable technology in the future. Technological transformation is evolutionary, despite talk of the current revolution in military affairs (RMA) based on information systems. One reason for this is "because new tools fit within an existing system."[12] Any demands on increasing the rate of transformation must take into account our legacy systems and organizations in order to balance current needs. Attempting to force revolutionary change could end in disaster with either full-fledged gridlock of the transformation process or, worse, losing a conflict over our vital interests due to technological failures.[13] Logistics, training and interoperability problems during modernization can be specifically likened to the gridlock on big city streets.[14] It is a matter of timing and flow control on a smaller scale to calculate and balance the impact a new system will have on the existing traffic. Without proper control the transformation process becomes congested and moves closer to gridlock.

Increasingly complex systems come with increasingly complex reliability and maintenance (R&M) issues. Typically, however, the logistics and maintenance support for new systems receives less attention than does design, production and fielding. Unresolved R&M issues result in poor mission capability of systems due to insufficient spares, long repair times and lack of field support. High-tech systems further increase the R&M problem by making it difficult for the user to detect and isolate faults that are beyond the system's internal test capability. The solution to this at the organizational unit level of maintenance is to remove the faulty component and replace it with a new or repaired component. Since the repair of high-tech components is increasingly beyond the capability of most military technicians, a system of "organizational to original equipment manufacture" (O to OEM) repair has been instituted. In this system, the end user removes and returns the component to its manufacturer for repair. If there are spares on site at the operational level, the system works. If there are not, the end user must wait for the next item to come out of the repair cycle. Department of Defense (DoD) budget constraints typically result in the supply system needing to catch up with newly fielded systems. The lack of spares, combined with the complexity of the component, and time for repair and delivery, increases the risk of failure associated with transformation. Without the proper logistic support for transformation technology, failures of complex systems will continue to multiply. Compounding the problem is the fact that we often base logistics support decisions on overly optimistic claims of reliability and repair turnaround by the manufacturers of high-technology systems. "Just-in-time logistics" is one example of optimism potentially leading to vulnerability.

The proliferation of multiple generations of systems during the transformation also increases interoperability problems between new and existing systems. Interoperability problems go beyond just the difficulty of one system working with another. The different generations,

modifications and upgrades multiply the number of equipment configurations end users are required to maintain and operate with limited manpower and support infrastructure. This further strains our training programs and the most obvious predetermined element, a limited budget.

The Budget: Gridlock's Root Cause

The greatest uncertainly associated with transformation is caused by the DoD budget. Limited funds will continue to force competition between the support of existing systems, fielding of those far into the acquisition process, and development of desired new systems. The more sunk costs involved in a system, the more likely it is we will field it whether or not it is compatible with our desired transformation end state. Cost overruns in both acquisition of new systems and support of old ones add further uncertainty to how the element of budget will influence transformation. Other considerations, including political ones, will result in these types of systemic mistakes continuing into the future.[15] The zero-sum nature of the defense budget will be most apparent during the introduction of large-scale missions and their associated systems, such as National Missile Defense. Any new mission areas undertaken in the future will compete with existing force structures in the constrained fiscal environment. Budget limitations also aggravate the military's difficulty competing, as a small customer compared to the private sector, in the information technology marketplace. It becomes increasingly difficult for the DoD to stay on the cutting edge of technology – it follows, rather than leads, the commercial sector, while potential enemies with the financial wherewithal compete as equals in the marketplace.

The CinC's Role in Transformation

The typical question for testing applicability at the CinC level is, "so what?"[16] If a CinC can't do anything about a problem it is only academic and his staff should spend their energies

elsewhere. The scenario of technology failure presents three broad and interrelated avenues of action at the CinC level, which can be likened to our recent national military strategy of "shape, respond, prepare now."[17] The CinCs can shape the transformation environment through their expectations and demands on the Services, they can respond to the risk of technology failure during transformation by training their forces for it, and they can prepare for the end-state of transformation by organizing now for dispersed, decentralized and self-synchronizing operations.

Shaping a Sustainable Transformation

A balanced approach to the transformation of our military services is required in order to reduce vulnerabilities inherent in the transformation process, especially those associated with logistics and own-force interoperability/compatibility issues. This means ensuring adequate logistics support and training to reduce the risk of transformation technology failure. The CinCs play a large role in our acquisition system, shaping the forces they need for present and future conflict. Demanding that personnel have been sufficiently trained with the technology they will bring to theater will go a long way in preventing technology failures caused by operator or support personnel errors. CinCs should also demand that systems complete "maturation development" in order to prevent, as much as possible, technology failures in the field. [18] Demanding maintainability instead of reliability statistics in order to forecast a system's future performance will help reinforce the maturation process. "The approach calls for a dedicated period of intense operation, data collection, and analysis…to detect and isolate design deficiencies by intensively operating the components in a fixed configuration within the environment where they will normally operate." These demands must, however, be backed up by avoiding the temptation to deploy the latest technology immediately. "Maturation development can be expected to delay the fielding of a new system or upgrade for a few years.

During the Cold War, procurement processes were highly compressed because of competition from the Soviet Union. With today's reduced risk, there should be less resistance to maturing systems before fielding them."[19] Despite this we continue to rush the fielding of immature systems without full logistic and training support, either because of a perceived critical need for a new capability or to support service acquisition goals. [20]

Responding to Transformation Failures

The likelihood of systemic technology failure is greatest during transformation. The limitations and complications of the transformation period, as previously discussed, will continue to make it difficult for the Services to train to such failures; they lack the time (due to high operations tempo) and money to train for operating with high-tech systems, let alone for operating without them. Yet, as mentioned earlier, we must be able to continue offensive operations regardless of the state of transformation or occurrence of technology failures. The alternative to training for system-wide technology failures during peacetime is to expect our servicemen and women to figure it out during actual operations. The choice should be clear.

Like indoor plumbing, information systems have become an infrastructure on which most of us depend but rarely think about or even understand. As in earlier cases, we cannot hang onto the remnants of the past as a backup for too long after the new technology matures. Training is about economic choices. Today's Sailors, Airmen, Marines and Soldiers are required to spend a large portion of their time learning how to use the technology specific to their assigned tasks. Each is a specialist in operating or maintaining something. As equipment becomes more complex, more time is required to learn how to operate and maintain it, leaving less time to learn why it works, how to question whether or not it is working correctly, and how to continue the mission without it. This reinforces the dependence on technology to the point that our forces are

helpless without it. The doctrine of "train how we fight" actually works against us if the technology fails because we were not able (or chose not) to train for such failures. A modern carrier battle group cannot conduct offensive operations without its C2 systems. Even basic skills like maneuvering depend on such systems. A generic definition of over-dependence on technology could be "the point at which it becomes too difficult to even attempt to train without." It is then a potential critical vulnerability which a competent adversary should seek every opportunity to attack.

The CinCs can mitigate this vulnerability by engaging their assigned forces with realistic training scenarios in which technology fails. Units forced to do without a critical piece of technology, such as GPS or an information network, may discover ways to mitigate these types of degradations during peacetime instead of during conflict. We must balance the training to avoid the over-dependence on technology and build the force's confidence that it can fight and win with or without it. Such training can also test the robustness of our force during organizational breakdown resulting from a disabling blow to our communications systems or hierarchical command structure. This brings us to the CinC's role in preparing for the future.

Preparing for Transformation Success (or Failure)

In their RAND study, Gompert and Lachow noted, "…networking mobilizes the intelligence of the *many* at the expense of control by the *few*. Consequently, the brilliance of leadership is measured increasingly by its ability to liberate the genius of the rank and file and to inspire that genius with a vision."[21] In the military that vision is in the form of a clear, concise and complete commander's intent to which the rank and file can apply its collective energy and genius. The process by which the rank and file focuses this energy on a common intent is self-synchronization.[22] The archenemies of self-synchronization are hierarchy and the human nature

that tends towards centralization and micro-management. Together they lead to what may be called “ego-centric warfare.” Its most basic symptom is the demonstrated belief (in actions, if not in words) that one assigned to a higher level of the hierarchy obviously knows better how to solve any problem than those assigned to lower levels.

> By climbing out of his tank, Lt. Devries gleaned one more crucial piece of data: the brush on the high ground where his bosses had stationed him was so dense that he didn't have a clear shot at the enemy. Consulting his computer again, Lt. Devries found what he thought was a better position about 500 yards away and radioed back for permission to move there. But his superiors, looking at the same digital display, told him there had to be an opening of some kind at his present spot. Frustrated, the lieutenant insisted that there wasn't. Stick to the plan, ordered his commander, Capt. Dane Acord.”[23]

Our information systems help create a more rigid top-down hierarchy that can result in stifled rather than enabled initiative. We have all bemoaned micro-management with the almost universal comment: “Just tell me what you want done, not how to do it.” This implies that what we need is clear commander’s intent before execution, not micro-management during execution. But in addition to achieving centralized control, our technology is reinforcing the human tendency for micro-management, enabling commanders and their staffs to also centralize execution. The challenge is to reap the benefits of technology while preventing centralized execution and being prepared in the event that technology fails at the critical time. Two possibilities for meeting this challenge include changing where we physically locate our staff officers and changing the way we assign information and communications bandwidth.

A central tenet of NCW is the dispersion of forces.[24] As we move toward those dispersed forces, we also increase the centralization of control, physically as well as procedurally. Decentralized execution with centralized control could be improved by reducing the size of operational commanders’ staffs at all levels, relocating some staff functions based on expertise to units in the next lower level in the hierarchy, units responsible for executing the commander’s

intent. In other words, disperse the staff amongst the nodes – not in the form of the German General Staff but as experts reporting to the unit to which they are physically attached, tasked with creating plans for submission to upper echelons. Such dispersal of staff functions could prevent those who would control and execute all operations from a central location from doing so, if only due to a lack of staff manpower. This begs the question, "Who will do the planning and oversight and myriad things staffs now do?" The same people will, working together via the connections made possible by technology, with the additional benefit of the expertise residing at the execution nodes, enabling continued operations in the face of technological failure.

In addition to providing a means of dealing with technology failure, decentralization also helps counter decentralized operations by the enemy. During the 1998 Army After Next Spring Wargame, the Red team decentralized its C2 structure. The recommended resolution to this tactic was for the U.S. to also decentralize. "Red issued detailed pre-war, mission-type orders to its major commands, thus permitting them to go on "autopilot" and move toward their objectives even when constant links to the Red NCA might not be possible."[25] This type of clear, concise and detailed commander's intent at each echelon in the hierarchy is critical if the organization is to continue in the face of a systemic technology failure, no matter its cause. Achieving it brings us to the next step in realizing self-synchronization – the use of bandwidth in a resource-constrained environment to reinforce decentralization.

It is possible to assign bandwidth access in a way that reinforces self-synchronization. Bandwidth assignments should be in support of two basic functions, communications and information. Information bandwidth should be relatively constant at all levels of the network hierarchy and through each phase of operations, allowing for demand access at the appropriate resolution and enabling a common operational picture. Conversely, communications bandwidth

assignments should change as the operation moves from the planning to the execution phase. The upper echelon should use the majority of its communications bandwidth at the beginning of an operation for communicating a detailed commander's intent, as discussed above. The farther one moves into the execution of an operation, the more the communications bandwidth requirement should shift away from the commander and to the units executing the operation. Video teleconferencing (VTC) is an example of a large bandwidth requirement that could be effectively switched from highest-level use during the planning phase to the lower levels during execution. Of course, the nature of ego-centric warfare is such that bandwidth (and information technology in general) has become a status symbol. It might be difficult to convince a commander or the staff to let the non-commissioned officers coordinating fires have the cool toys instead, but that is exactly what the CinCs need to do.

Conclusion

This paper is about preparation, not prediction. Predictable and unpredictable difficulties lurk around every turn on the path to full spectrum dominance; we will never entirely prevent Clausewitzian friction. Preparing for flexible responses to the uncertainties caused by our systems of government, acquisition, training and operations, and to those caused by the environment our forces will operate in, is important as we transform to the joint force of the 21st Century. We must ask the question, "what if our technology fails?" now, before suffering the consequences on the battlefield.

Simply stating in our joint doctrine and joint vision statements that we will have full-spectrum dominance will not make it so. We risk being lulled into complacency by technology's promises, especially during the transformation period. Technology is subject to failure even

during peacetime when nobody is actively trying to disable it; the rigors of wartime operations only make it more susceptible to failure. Technology trade, an important peacetime economic interest, facilitates access of dual-use technologies by potential adversaries who can use it against us, further eroding our assumed technological superiority. During war our forces must be able to continue fighting in spite of such failures.

I do not advocate a return to the good old days. We should continue to apply technology to our advantage wherever it is sensible to do so. Given the forces that shape transformation, however, failure of some of our most critical technologies in future conflict is at least feasible. It is incumbent on us to prepare for such eventualities. The CinCs should ask the following questions to ensure a successful, balanced transformation:

- Are we demanding the premature deployment of technological systems without due consideration for logistic, interoperability and training issues?
- Are we conducting training that accounts for technology failure, whether caused by competent adversary or transformation problems?
- Are we organized for success in case of both network centric operations or degraded operations due to systemic technology failure, with a structure that supports self-synchronization while hindering micro-management?
- Can we still fight and win if key technological systems fail?

Not every conflict in which we find ourselves will offer the luxury of pulling out when technology failure forces us to resort to more primitive techniques. If we are fighting for a vital national interest, we must be able to continue the offensive fight with or without some of the systems on which we have become so dependent.

On the strength of one link in the cable,
Dependeth the might of the chain.

Who knows when thou may’st be tested?
So live that thou bearest the strain! [26]

NOTES

[1] Milan N. Vego, Operational Warfare, (Newport, RI: Naval War College, December 2000), 309.

[2] Joint Chiefs of Staff, Joint Vision 2020, (Washington, DC: USGPO, June 2000), 1.

[3] Critical vulnerabilities are defined as critical strengths or weaknesses which "are directly related to the enemy's center of gravity and are vulnerable to attack by friendly forces." Joint Military Operations Department, Syllabus and Study Guide for Joint Military Operations, (Newport, RI, 2001), 53.

[4] Science and technology and asymmetric warfare are among the eight issues cited by the National Intelligence Council as "key uncertainties" and have direct implications for our technology-bound transformational military. "What we do not know about the S&T revolution, however, is staggering." National Intelligence Council, Global Trends 2015: A Dialogue About the Future With Nongovernment Experts, (December 2000), 13-15.

[5] For an enlightening article on traffic flow see Stephen Budiansky, "The Physics of Gridlock," The Atlantic Monthly, December 2000, 20-24.

[6] Peter Schwartz, The Art of the Long View (New York: Doubleday 1991), 105.

[7] Based on counts made from Department of the Army, Weapon Systems 1986, (Washington DC: USGPO, 1986, and Department of the Army, Weapon Systems 2000, (Washington, DC: USGPO, 2000). Of course all weapons systems are based on technology but for the purposes of the current transformation, information systems and related technologies are germane for this comparison. I arbitrarily used direct enemy contact as a means of separating technology-oriented from basic systems. This basically excludes tanks, guns, aircraft and missiles. Precision guided munitions could easily be counted as technology-dependent but complicates the process and their inclusion would only strengthen the point.

[8] National Intelligence Council, Global Trends 2015: A Dialogue About the Future With Nongovernment Experts, (December 2000), 57.

[9] This conflict of interest is given considerable attention in our national security strategy, which notes, among other things, "computer technology is an area where the application of export controls must balance our national security concerns with efforts to promote and strengthen America's competitiveness." President, A National Security Strategy for a Global Age, (Washington, DC: The White House, December 2000), 33-34.

[10] Schwartz, 111.

[11] When I attended the Force Over-the horizon Track Coordinator (FOTC) Course at Fleet Combat Training Center in San Diego in 1993, our instructor, Reed Popovich, taught us to

imagine a flashing neon sign over our computer screen that read, "THIS IS A LIE," to remind us that what appeared on our screens was not ground truth and that we should not blindly trust the technology.

[12] Schwartz, 148.

[13] I think using the term "revolutionary" to describe anything we are currently involved with is premature; that is for history to decide. Our arrogance will be harshly judged if the current RMA is really only a trigger for a true revolution in how states wage war (i.e. one that avoids our technological superiority).

[14] The timing of stoplights on city streets is based on the length of a block, the length of each platoon of vehicles and the intended driving speed. Basically, gridlock occurs when the platoon of vehicles becomes longer than the block it is traveling on and backs up into the next intersection behind the light it is stopped at.

[15] This is so despite current discussions of rapid and sweeping changes. For a summary of what is being considered, see Tom Bowman, "Pentagon Faces Transformation," Baltimore Sun (March 13, 2001). Accessed from Defense Primary Current News Service at <http://ebird.dtic.mil> [13 March 2001].

[16] "Does your paper pass the 'so what' test by the CinC's" is a common question during the JMO paper topic selection process at the Naval War College. The complimentary question is, "What can the CinC do about it?"

[17] The elements "shape, respond, prepare now" are borrowed from Joint Chiefs of Staff, National Military Strategy of the United States of America, (Washington, DC: 1997).

[18] "The goal of maturation development is the delivery of full designed performance of the weapon system under mission conditions and the rapid restoration of full design performance when malfunctions occur." John Dumond and others, Maturing Weapon Systems for Improved Availability at Lower Costs, (Santa Monica, CA: RAND, 1994), xii-xv.

[19] Ibid., xiii.

[20] As the staff maintenance and logistics officer for a patrol wing, and member of the P-3C/EP-3E Fleet Support Team, I was involved in decisions ranging from daily aircraft operations and maintenance to life cycle management, including the fielding of the Anti-surface warfare Improvement Program (AIP), the most recent major upgrade to the P-3C aircraft. We sent the very first three AIP aircraft assigned to the East Coast directly from the factory to an operational deployment. This decision was based in large part on the necessity to win CinC support for the upgrade in the upcoming budget cycle. From then on, we continued to keep every mission capable AIP aircraft deployed, with no operating assets for training at home base. Additionally, the aircraft was knowingly fielded and deployed before its integrated logistics support was in place. This transformation of the P-3C was further aggravated when operation ALLIED FORCE

began, forcing subsequent squadrons deploying in support of the operation to send aircrews to train in theater, for lack of training assets at home. We were on both the verge of gridlock and potential operational failure.

[21] David C. Gompert and Irving Lachow, "Transforming U.S. Forces: Lessons from the Wider Revolution," (RAND, National Defense Research Institute), Accessed at <http://www.rand.org/publications/electronic/force.html> [10 Apr 2001].

[22] Self-synchronization is defined as "units within a force use common information, the commander's intent, and a common rule set – or doctrine – to self-organize and accomplish the commander's objectives." Naval War College Faculty, Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age, Smooth Draft, (Newport, RI: Joint Military Operations Department, U.S. Naval War College, 2000), 9.

[23] Greg Jaffe, "The Army Bets Its Battlefield Success on Soldiers Armed with Better Data," Wall Street Journal, 30 March 2001, p. 1. Accessed from Defense Primary Current News Service at <http://ebird.dtic.mil> [30 March 2001].

[24] "The first key concept is the use of geographically dispersed force." David S. Alberts, John J. Garstka, Frederick P. Stein, Network Centric Warfare, (Washington, DC: CCRP, 1999), 88.

[25] Walter L. Perry, Bruce R. Pirnie and John V. Gordon IV, Issues Raised During the Army After Next Spring Wargame, (Santa Monica, CA: Rand, 1999), 19-20.

[26] Fifth stanza from Admiral R. A. Hopwood, R.N. (Ret.), "The Laws of the Navy," in Reef Points 1981-82, (Annapolis, MD: United States Naval Academy, 1981), 40-44.